UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

BESSEMER SYSTEM FEDERAL CREDIT UNION, on behalf of itself and its members,

Plaintiff,

vs.

FISERV SOLUTIONS, LLC, f/k/a FISERV SOLUTIONS, INC., and FISERV, INC.,

Defendants.

Case No. 2:19-cv-00624-RJC

BESSEMER'S OBJECTIONS TO SPECIAL MASTER'S REPORT AND RECOMMENDATION REGARDING MOTIONS TO COMPEL DISCOVERY

Charles J. Nerko (NY 4764338)
Kevin D. Szczepanski (NY 2720118)
Benjamin M. Wilkinson (NY 4927661)
BARCLAY DAMON LLP
80 State Street
Albany, NY 10020
(518) 429-4200
cnerko@barclaydamon.com
kzczepanski@barclaydamon.com
bwilkinson@barclaydamon.com

Richard J. Parks (PA 40477)
PIETRAGALLO, GORDON, ALFANO,
BOSICK & RASPANTI, LLP
7 West State Street, Suite 100
Sharon, PA 16146
(724) 981-1397
rjp@pietragallo.com

Counsel for Plaintiff
Bessemer System Federal Credit Union

Pursuant to the Order Approving Discovery Special Master (Dkt. 195), Plaintiff Bessemer System Federal Credit Union, a federally chartered not-for-profit credit union ("Bessemer"), hereby objects to portions of the Report and Recommendation dated June 13, 2023 ("R&R") issued by Special Master Mark D. Shepard, which addresses the parties' discovery motions, including the appropriate scope of discovery.

As detailed below, Bessemer objects to the following recommendations contained in the R&R which:

(1) Inappropriately limit the scope of appropriate discovery solely to documents and communications and documents involving or relating to Bessemer;

(2) Deny Bessemer's motion to compel Fiserv to produce security audit documents and communications;

(3) Deny Bessemer's motion for a protective order regarding preservation of Bessemer voicemails;

(4) Deny Bessemer's motion to compel privilege logging by Fiserv beyond June 30, 2019;

(5) Deny Bessemer's motion to compel FFIEC Examination Reports; and

(6) Grant Fiserv's motion to compel Bessemer to provide information about the expert Bessemer retained—after it commenced litigation against Fiserv—to assess the sufficiency of Fiserv's information-security controls for its online "Virtual Branch" and "Charlotte" banking platforms used by Bessemer and other credit-union members.

Procedural History

Throughout this litigation, the parties have significantly differed on a number of discovery issues, including the appropriate scope of discovery relevant to the claims defense in this matter, as further described below. In late 2021, the parties held several meet and confers to address their discovery disputes, but were unable to reach an agreement on a number of subjects, which prompted the instant motions to compel.

On December 15, 2021, Fiserv filed its Motion to Compel Discovery Relating to Bessemer's Security Review. (Dkt. 138). On January 31, 2022, Bessemer filed five (5) separate discovery motions: A Motion to Compel Fiserv to Provide a Privilege Log for Communications After June 30, 2019 (Dkt. 154); a Motion to Compel Fiserv to Provide Responses to Bessemer's Second Request for Production (Dkt. 157); a Motion to Compel Fiserv to Produce Documents Related to Security Audits (Dkt. 161); a Motion for Protective Order Regarding Fiserv's Request for Bessemer's Voicemails (Dkt. 164); and a Motion for Protective Order Regarding Fiserv's Request for Security Review Discovery (Dkt. 167).

On June 7, 2022, the Court appointed Mark D. Shepard to serve as the discovery Special Master and the referred the motions to him. (Dkt. 194). The parties held multiple conferences with Special Master Shepard in attempt to resolve any discovery disputes and began exchanging documents responsive to the parties' respective discovery demands.

On March 22, 2023, the parties submitted supplemental briefing regarding the pending motions and were permitted to raise any new issues by way of letter brief. On May 16, 2023, Special Master Shepard held oral arguments regarding the pending motions and on June 13, 2023, Special Master Shepard issued an R&R regarding the pending discovery motions. (Dkt. 209).

Objections to Certain Recommendations

1. **Bessemer's request for documents related to other Fiserv clients, systems, services (R&R Section III(A)(5))**

Bessemer objects to the portion of the R&R which recommends that the scope of discovery in this matter be artificially limited to Fiserv's documents and communications directly involving or referencing its relationship with Bessemer. (Dkt. 209, p. 9). Specifically, Bessemer objects to any limitation on Fiserv's obligation to produce documents and communications relevant to

Bessemer's fraudulent inducement claim that demonstrate Fiserv's overall awareness of security deficiencies prior to entering into the Master Agreement with Bessemer.

The parties possess significantly different views regarding the appropriate scope of discovery in this matter. Fiserv frames this case as a simple breach-of-contract case and seeks to ignore Bessemer's other claims. This approach attempts to unduly narrow the scope of discovery to artificially limit the issues at hand and deprive Bessemer access to necessary proof. In response to Bessemer's discovery requests, the majority of Fiserv's responses contain objections that Bessemer's RFPs seek information beyond that which is directly related to or involving Bessemer. Thus, Fiserv proposes to limit the majority of the communications and documents produced in discovery to *only* those with Bessemer.

In contrast, Bessemer should be entitled to take discovery on all of its claims that survived Fiserv's motion to dismiss. Those include not only its breach-of-contract claim, but also its claims for fraudulent inducement, bailment, and misappropriation of trade secrets under the PUTSA and DTSA. The Court also permitted Bessemer to seek punitive damages, necessitating reasonable discovery to prove each and every element of its claims—plus the "willful, wanton, and reckless" element necessary to establish its entitlement to punitive damages. Indeed, the Second Amended Complaint ("SAC") and this Court's decision on Fiserv's motion to dismiss demonstrate that this case extends beyond a mere contract dispute. Accordingly, discovery must proceed on a correspondingly broad and appropriate basis.

In response to multiple letter briefs on the subject, the R&R recommends limiting the scope of discovery such that "Bessemer's Motion to Compel production of documents unrelated to Bessemer and/or the services supplied to Bessemer should be denied" with a limited exception. (Dkt. 209, p. 9).

Bessemer objects to this portion of the R&R on the basis that it precludes Bessemer from taking discovery directly related to its claim for fraudulent inducement of the Master Agreement. The R&R improperly precludes discovery of documents concerning what Fiserv knew about deficiencies in its systems—and when Fiserv knew it—effectively precluding discovery of the misrepresentation and scienter elements of Bessemer's fraud claim.

As the Court is aware, Bessemer's fraudulent inducement claim is predicated on Fiserv's misrepresentations regarding the existence and nature of security controls it placed on its Virtual Branch and Charlotte systems, which were Fiserv's online banking platforms provided to Bessemer. Specifically, in a February 12, 2012 email, and other communications, Fiserv falsely represented that its Virtual Branch authentication process had security controls that were compliant with FFIEC cybersecurity requirements. Bessemer's fraudulent inducement claim survived Fiserv's motion to dismiss. (Dkt. 69). Thus, Bessemer seeks to take discovery in support of this claim, which includes information and documents regarding Fiserv's awareness of its security authentication procedures (or lack thereof) ***prior to the February 2012 email*** at issue and regardless of whether relevant documents or communications specifically involved Bessemer. In other words, Bessemer is entitled to take discovery regarding Fiserv's knowledge of its authentication, whether that complied with FFIEC requirements, and *when* it acquired that knowledge. This issue is vital to proving that Fiserv was aware that the statements contained in the February 2012 email to Bessemer were knowingly false. *See Joyce v. Erie Ins. Exch.*, 74 A.3d 157, 166-167 (Pa. Super. 2013).

By way of example, Bessemer's Requests Nos. 43-53 seek documents regarding cyber threats, security vulnerabilities, and data breaches known by Fiserv, Fiserv's responses to these events, and Fiserv's policies and procedures to address them. These requests are clearly relevant to Bessemer’s fraudulent inducement claims, as well as punitive damages allegations, as they aim to establish whether Fiserv was aware of specific security vulnerabilities at the time of contracting with Bessemer, but failed to take action to remedy them or made misrepresentations regarding its security capabilities. In response to each request, Fiserv’s responses contain objections that the request is overly broad and unreasonable because they inquire about events that may not have impacted Bessemer. Similarly, Fiserv’s search terms of its own e-discovery are limited to those explicitly involving Bessemer. Put simply, if “Bessemer” does not appear within the document, Fiserv has refused to search and produce that document—no matter how relevant it may be to the claims in this case.

The end result of applying Fiserv’s methodology, which the R&R seeks to adopt, is that if the communication does not involve or reference Bessemer, but discusses a data breach, security vulnerability or authentication issue relevant to Bessemer’s fraudulent inducement claim, then Fiserv will seek to withhold that information. In doing so, Fiserv impermissibly seeks to limits discovery that demonstrates its awareness of security vulnerabilities that existed within its systems—even though this is showpiece evidence indispensable to Bessemer’s fraudulent inducement claim. Limiting documents bearing on Fiserv’s knowledge to only those involving Bessemer would largely preclude discovery of the scienter element of Bessemer’s fraud claim.

Moreover, the R&R’s recommendation to limit discovery solely to Bessemer grossly overlooks the manner in which Fiserv may have received notice of security deficiencies, which is critical to Bessemer’s fraudulent inducement claim. Bessemer is entitled to receive discovery regarding evidence of the same or similar deficiencies in information security controls in the online Virtual Branch and Charlotte banking systems as they bear on Fiserv’s FFIEC compliance. Fiserv may have been made aware of security vulnerabilities and security incidents by Bessemer, other credit-union customers, or even through its own internal investigations, security reviews, maintenance, or upgrades to these systems. Limiting discovery to only those documents that happen to involve Bessemer is tantamount to precluding discovery of the very fraud claim that this Court has permitted to proceed to discovery.

Applying the R&R's discovery scope, Fiserv could have learned of a security defect in 2008, 2009, 2010 through an incident involving another customer—or discovered and discussed one internally—but because that incident did not involve Bessemer, Fiserv is not required to produce those documents. Indeed, under the R&R, none of Fiserv's internal documents concerning defects or vulnerabilities, or FFIEC compliance issues with Virtual Branch are subject to discovery unless they somehow reference Bessemer. This evidence is fundamental to Bessemer's fraudulent inducement claim. The key inquiry is Fiserv's knowledge of the defects in the system. Thus, the R&R's recommendation severely limits discovery such that Bessemer is not in a position to prove its fraudulent inducement claim.

The R&R's recommendation regarding the scope of discovery also contradicts the parameters of discovery set forth in the R&R. In discussing the relevant and appropriate areas for discovery, the R&R lists "the communications, interactions and documents relating to the negotiation of…[the] Agreement." (Dkt. 209, p. 5). This is exactly what Bessemer seeks to discover—the validity and accuracy of the statements in the February 2012 email in the lead up to the execution of the Master Agreement. The only means to do is by obtaining discovery on Fiserv's knowledge of its FFIEC compliance—regardless of whether that had to do with Bessemer.

Based on the foregoing, Bessemer respectfully requests that the Court grant Bessemer's motion to compel such that Fiserv is required to search and produce documents related to the FFIEC compliance and authentication—regardless of whether those documents involve or reference Bessemer. This includes design of Virtual Branch and Charlotte and their authentication protocols and how Fiserv complied with FFIEC guidelines. All documents related to this discrete issue should be searched and produced by Fiserv.

2. Bessemer's motion to compel documents related to other Fiserv clients and security issues (R&R Section III(A)(3))

Bessemer objects the R&R's recommendation that the Court deny Bessemer's motion to compel documents and information related to security audits conducted by Fiserv or notices regarding security deficiencies related to Fiserv products. (Dkt. 209, pp. 7-8). By way of background, Bessemer's underlying motion sought to compel Fiserv to produce security audit documents responsive to Request Nos. 11, 45, 139, 140, 144, 149, 183 and 184 in Bessemer's First Request for the Production of Documents. (Dkt. 161). These requests, which are reproduced below, sought various documents related to Fiserv's security measures and plans:

> **Request No. 11:** Documents concerning the research, development, testing and evaluation of the Services at Issue, including any beta tests, focus groups, audits, monitoring, or other analysis (whether prior to or after launch).
>
> **Request No. 45:** Documents concerning investigations undertaken by Fiserv concerning any Cyber Threats, Security Vulnerabilities, or Data Breaches, including documents reflecting the method or means by which any unauthorized third party or third parties may obtain access to systems, the length of time any unauthorized third party or third parties may have been able to access systems, and the information any unauthorized third party or third parties may have been able to access, view, copy or otherwise obtain.
>
> **Request No. 139:** Documents concerning internal and external audits, assessments, and investigations of Fiserv's data security policies, procedures and practices.
>
> **Request No. 140:** Documents concerning Fiserv's risk assessment policies, procedures, and actual practices, including risk assessment reports (including drafts).

> **<u>Request No. 144:</u>** Documents concerning methods to ensure the confidentiality, security, availability and integrity of Bessemer's Member Information and Bessemer's Member Information Systems.
>
> **<u>Request No. 149:</u>** Documents concerning any analysis, assessment, test, audit, evaluation, implementation, monitoring review, and the sufficiency of Your attempts to comply with, and non-compliance with, FFIEC requirements.
>
> **<u>Request No. 183:</u>** Documents concerning audit documents, inclusive of any audit documents themselves, Fiserv was required to maintain pursuant to Sections 4(a), 4(b), 4(d) and 4(h) of the Master Agreement, including documents concerning the allegations in SAC 141-144.
>
> **<u>Request No. 184:</u>** Documents concerning Fiserv' response to Bessemer's audit.
>
> **<u>Request No. 186:</u>** Documents concerning Fiserv's response to Bessemer's audit, including communications concerning interim drafts of Fiserv's September 11, 2018 audit response.

(Dkt. 162). Bessemer's document requests regarding Fiserv's security audits are highly relevant because the crux of Bessemer's claims involve Fiserv's failure to safeguard Bessemer's records, which exposed Bessemer's members to potential identity theft and fraud. [1] (Dkt. 48, ¶¶ 26-79). They are also relevant in connection with Bessemer's fraudulent inducement claim regarding whether Fiserv had adequate security precautions in place prior to making representations to Bessemer regarding their compliance with FFIEC standards. One manner in which Fiserv would be aware of such security problems is through their security audits of their systems. Fiserv's awareness of the pre-existing security problems—and its remedial action (or lack thereof)—are of vital significance to Bessemer's claims.

[1] Fiserv was also required to provide security audit documents under the terms of the Master Agreement. The Master Agreement explicitly required Fiserv to disclose to Bessemer: "audit reports, summaries of test results or equivalent measures" taken by Fiserv to assess the sufficiency of its information security program in protecting Bessemer's member information and records. (Dkt 48, ¶ 140; 48-2, Section 4). Thus, the failure to produce these documents is relevant to Bessemer's breach of contract claim.

Fiserv objected to these requests on the basis that Bessemer's demands are overly broad and burdensome. (Dkt. 163-2). In particular, Fiserv's responses sought to limit their potential production of documents to those which related to the services and products Fiserv provided to Bessemer—rather than documents and reports related to audits that impact Fiserv's overall security services. (*Id.*). As a result, Bessemer moved to compel Fiserv to provide less narrowed responses to the aforementioned requests.

The R&R recommends that Fiserv produce any security incident reports from 2011 for Charlotte and Virtual Branch products. (Dkt. 209, p. 8). The R&R notes that Fiserv produced the security incident reports related to those systems for 2012 through 2014. (*Id.*). It also directed the production of Charlotte and Virtual Branch meeting minutes for 2011. (*Id.*). However, R&R recommends denying Bessemer's request for any other related documents. For the reasons that follow, the Court should reject this recommendation and grant Bessemer's motion to compel.

At the outset, the R&R oversimplifies Bessemer's requests and thereby inappropriately narrows discovery on this subject. Bessemer's requests did not merely seek the incident reports for Charlotte and Virtual Branch. Rather, the requests sought all documents associated with the research and testing of the security of the services provided, Fiserv's investigations into data security, and Fiserv's' analysis to comply with FFIEC security requirements, among other subjects. For example, Request No. 149 seeks documents concerning any analysis, assessment, test, audit, evaluation, implementation, monitoring review, and the sufficiency of Fiserv's attempts to comply with, and its non-compliance with, FFIEC requirements. This request goes beyond mere incident reports and requires production of internal memoranda and communication, if any, regarding Fiserv's efforts to comply with FFIEC requirements. As noted above, Fiserv's awareness of its own security vulnerabilities, and the documents and communications that would reflect that knowledge, are clearly relevant to its claims of fraudulent inducement and breach of contract. Limiting Bessemer's discovery to merely security incident reports does not provide Bessemer adequate discovery.

In addition, the R&R arbitrarily limits the production of security incident reports to 2011. The R&R reasons that because Mr. Reynold's email to Bessemer regarding FFIEC compliance occurred in 2012, Fiserv should only be required to produce incident reports going back to 2011. However, the R&R recognizes that Bessemer is "entitled to explore Fiserv's knowledge regarding any report defects or shortcomings in the systems and services ultimately supplied to Bessemer." (Dkt. 209, p. 8). To that end, the purpose of Bessemer's request for production was to explore Fiserv's knowledge of its own vulnerabilities prior to entering into the Master Agreement with Bessemer. Permitting Bessemer discovery on this subject for merely a one year look back to 2011 arbitrarily limits Bessemer's discovery. A more appropriate and proportional look back point would take into account the point at which Fiserv implemented the Virtual Branch and Charlotte systems, and the point at which Fiserv developed and implemented its FFIEC controls for those systems. Bessemer is entitled to discovery of the documents and communications that reflect Fiserv's decision making, analysis and internal communications regarding security vulnerabilities, incidents, and breaches, if any, from that point forward. There is no rational basis—in the record or otherwise—to artificially limit the look-back period to 2011.

Further, Bessemer is entitled to discovery of documents regarding complaints of security vulnerabilities from other customers and discussions of security deficiencies more generally—not just incidents or complaints involving Bessemer. (*See* Request No. 45). It is highly unlikely that Fiserv's security controls as a whole would be reflected solely in documents referencing Bessemer. It seems equally, if not more, likely that documents pertaining to security issues with Fiserv's

Virtual Branch or Charlotte banking systems—including the degree to which these systems comply with FFIEC requirements—would *not* reference Bessemer or any other Fiserv customer Given this, the R&R's artificial limitation on production to only those documents pertaining to Bessemer is tantamount to precluding discovery on Bessemer's fraudulent inducement and breach of contract claims. As argued above, the key inquiry to those claims is what Fiserv knew regarding the security of its systems and what, if anything, Fiserv did to address these issues both before and after the parties entered into the Master Agreement.

In addition, Bessemer is entitled to take discovery on its punitive damages allegations, which allege that Fiserv's misconduct and repeated security failures are part of a pattern that harmed Bessemer and other financial institutions, and ultimately, scores of consumers (Dkt. 48, ¶¶ 204-205), and Fiserv failed to implement proper security controls for Bessemer despite having knowledge of prior similar data breaches that affected other Fiserv customers (*id.* ¶¶ 51-52, 202, 207). Thus, discovery on Fiserv's security practices generally, and its response to other data breaches, are relevant here because they show Fiserv's state of mind, knowledge of proper security controls and their implementation, notice of security problems, the extent of public harm, and the quantum of punitive damages needed to deter Fiserv from committing similar incidents in the future. Accordingly, Fiserv should be ordered to produce the requested security audit documents without further delay.

3. Motion to compel privilege logging by Fiserv beyond June 30, 2019 (R&R Section III(A)(1))

Bessemer also objects to the portion of the R&R which recommends denying Bessemer's motion to compel Fiserv to complete privilege logging beyond June 30, 2019. (Dkt. 209, p. 6).

To briefly recap the relevant factual background, when Bessemer terminated its contractual relationship with Fiserv, it demanded that Fiserv return Bessemer's records. While Fiserv eventually returned a copy of Bessemer's records, Fiserv did not dispossess itself of those records. Rather, Fiserv continues to retain Bessemer's records and asserted that it owns them. (Dkt. 48, Ex. 29). As a result, Bessemer's bailment and declaratory judgment claims seek redress for Fiserv's ongoing and improper retention of Bessemer's records after Fiserv was terminated as a vendor. In particular, Bessemer's bailment claim seeks money damages and injunctive relief related to Fiserv's interference with Bessemer's superior possessory rights in its account records. (Dkt. 48, ¶¶ 293-300, p. 90 demand for relief (iv)). Bessemer's declaratory judgment claim seeks a declaration from the Court that Fiserv does not own Bessemer's member information and has no legitimate purpose in asserting ownership over and "continuing to possess" Bessemer's member information. (*Id*. at ¶¶ 329-336). The Court has already held that Bessemer sufficiently set forth claims for both bailment and declaratory relief related to Fiserv's ongoing retention and claimed ownership of Bessemer's records and denied Fiserv's motion to dismiss these claims. (Dkt. 69 at 34, 52). Bessemer is thus entitled to take discovery on these claims.

The R&R recommends denying Bessemer's motion on the basis that creates an unnecessary burden on "both parties" with little benefit. (Dkt. 209, p. 6). On the contrary, Bessemer is entitled to a privilege log of all communications regarding the disposition of Bessemer's records in connection with its bailment and declaratory judgment claims. Bessemer's bailment and declaratory judgment claims seek redress for Fiserv's *ongoing* and improper retention of Bessemer's records after Fiserv was terminated as a vendor. Thus, attorney-client communications after June 30, 2019, particularly those communications regarding the disposition of Bessemer's records that Fiserv claims it owns, must be logged in order for Bessemer to adequately evaluate Fiserv's assertions of privilege. The R&R wholly overlooks the particular significance of Bessemer's request for logging in connection with the ongoing nature of the bailment and declaratory judgment claims and must be rejected.

4. Bessemer's motion for Protective Order regarding voicemails (R&R Section III(A)(1))

Bessemer further objects to the portion of the R&R denying Bessemer's motion for a protective order regarding the preservation of Bessemer voicemails. (Dkt. 209, p. 9). In response to Fiserv's discovery requests regarding voicemails that Fiserv personnel left for Bessemer regarding the security review and deconversion from Fiserv, Bessemer sought a protective order declaring that Bessemer was not required to produce voicemails on the basis that voicemail preservation is not required under the Court Court's Model Stipulated Order Re: Discovery of Electronically Stored Information for Standard Litigation, which is incorporated into the Western District of Pennsylvania's Local Rules.[2] (Dkt. 164). Bessemer's responses to Fiserv's discovery requests otherwise admitted the timing and contents of the voicemails left by Fiserv. In response, Fiserv opposed Bessemer's request for a protective order, but did not move to compel. (Dkt. 173).

The R&R recommends that Bessemer must provide a response to Fiserv regarding whether any such voicemails exist to produce *and to produce* those related to security review.[3] (Dkt. 209, pp. 9-10). Bessemer objects to this finding for the reasons that follow.

First, the R&R contradicts the express provision of the Court's Model Stipulated Order without providing any basis to do so. Neither the R&R nor Fiserv's opposition offers any reason to deviate from the default provision in this Court's Model Order.

[2] https://www.pawd.uscourts.gov/sites/pawd/files/lrmanual20181101.pdf, p. 113.

[3] The R&R does not require Bessemer to identify and produce voicemails related to deconversion, which Bessemer does not object to. (Dkt. 209, p. 10).

Next, the R&R lacks proportionality. *H.J. Heinz Co. v. Starr Surplus Lines Ins. Co.*, 2015 U.S. Dist. LEXIS 184222 at *11-12 (W.D. Pa. 2015). The burden on Bessemer to unearth the content of voicemails far outweighs any marginal benefit of their preservation and production. Bessemer would have to incur a significant cost to search and produce voicemails. *H.J. Heinz Co.*, 2015 U.S. Dist. LEXIS 184222 at *14 (denying motion to compel voicemails stored on system configured to automatically delete voicemails after 14 days). Bessemer has already admitted the contents and timing of the voicemails and thus, the evidentiary value of the voicemails themselves is negligible. As such, Bessemer should be relieved of the burden of continued voicemail preservation—consistent with the Court's default preservation rules and proportionality principles.

Finally, the R&R's ruling on this issue goes well-beyond the requested relief of Bessemer's initial motion for a protective order. Rather than merely recommending to grant or deny Bessemer's request for a protective order, the R&R *sua sponte* directs the identification and production of voicemails, despite the fact that Fiserv never requested such relief. In its own words, "Fiserv has not yet demanded (and may never demand)" production of voicemails, "Fiserv has not pressed for production of any voicemails now," and Fiserv also concedes that other discovery "may obviate any need for Fiserv to request production of voicemails in the future." (Dkt. 173, pp. 4, 14-15). As there has never been a pending motion to compel voicemails, there is no extant need for Bessemer to identify and produce them, as the R&R directs. Accordingly, Bessemer respectfully requests that the Court grant Bessemer's request for a protective order or, in the alternative, refuse to adopt the R&R's recommendation that Bessemer identify and produce voicemails related to the security review.

5. Bessemer's motion to compel FFIEC reports (R&R Section III(A)(7))

Bessemer objects to the R&R's recommendation to deny its motion to the extent it sought to compel Fiserv to produce FFIEC Examination Reports for Virtual Branch. (Dkt. 209, p. 10). Bessemer sought FFIEC reports regarding Virtual Branch in connection with its claims for breach of contract and fraudulent inducement. These reports would demonstrate Fiserv's compliance with FFIEC standards (or lack thereof) during its relationship with Bessemer. Fiserv objected to Bessemer's demands for same on the basis that the reports are protected by FFIEC examination privilege.

The R&R recommends that Bessemer's motion be denied on the basis of the privilege and directs Bessemer to seek these documents through subpoena or FOIA request. Bessemer objects because nothing precludes Fiserv from producing any non-final reports prepared by Fiserv. Non-final reports that were not submitted to the FFIEC are not subject to the same privilege and are therefore discoverable.

6. Fiserv's motion to compel security reviewer information (R&R Section IV(B))

Bessemer objects to the portion of the R&R granting Fiserv's motion to compel Bessemer to provide information regarding the security expert Bessemer retained to aid in providing legal advice with respect to claims against Fiserv based on deficiencies in the information-security controls in its Virtual Branch and Charlotte systems. (Dkt. 209, pp. 18-19). By way of background, Fiserv's motion to compel sought the identity and documents regarding Bessemer security expert, which were withheld by Bessemer on the basis that Fiserv's requests sought to invade attorney work product and constituted a violation of the consulting expert privilege. (Dkt. 138).

The R&R recommends granting Fiserv's request for information regarding Bessemer's security expert on basis that Bessemer relied on the expert's actions as part of its claims and the security reviewer's action serve as the central basis for Fiserv's counterclaims. (Dkt. 209, p. 18). The R&R also concludes that the security experts's identity and actions are not protected by consulting expert privilege under Rule 26(B)(4)(D). (*Id.*).

Bessemer initially objects to the R&R's recommendation on the basis that the R&R plainly ignores that the discovery sought by Fiserv constitutes attorney-work product. After commencing litigation in state court against Fiserv in May of 2018, Bessemer's litigation counsel engaged a security expert to evaluate the claims Bessemer was prosecuting in the state court action. (Dkt. 149, ¶¶ 10-11). The expert's retainer agreement, executed in September of 2018, bears all the hallmarks of work product. (Dkt. 149-1). The expert was engaged by Bessemer's litigation counsel and required to communicate with counsel. (Dkt. 149-1; 149, ¶¶ 15-16). The retainer agreement explicitly notes that the security expert was being retained by counsel in connection with existing litigation to assist in providing a legal analysis of the claims Bessemer was pursuing. (Dkt. 149-1). The expert's scope of work was also limited solely to litigation activities. (*Id.*).

Fiserv's discovery requests regarding the security expert seek both mental impressions and work product regarding the legal investigation of Bessemer's claims *after* Bessemer commenced litigation. For example, Fiserv's Interrogatory No. 10 requested a detailed description of the "individual steps" taken during the security review and reports and other analysis produced; RFP No. 24 requested "[a]ll documents relating to the Security review"; RFP No. 25 requested the "data, reports, or analysis generated" by the expert engaged by litigation counsel; and RFP Nos. 27 and 28 sought "[a]ll documents reflecting or relating to any communications…relating to the security review." These requests seek to obtain the technical expertise and advice provided by the security expert and used by Bessemer's counsel to develop legal advice for its client as well as the mental impressions of counsel contained in any related analysis and communication. Thus, they are clearly shielded by the work product doctrine. *See Genesco, Inc. v. Visa U.S.A., Inc.*, 296 F.R.D. 559, 581 (M.D. Tenn. 2014) (denying motion to compel discovery related to a cybersecurity consultant engaged by counsel—recognizing that the work product doctrine "attaches to an agent's work under counsel's direction" and cybersecurity consultant was retained in contemplation of litigation, as demonstrated by the language of the retainer agreement).

The R&R appears to reason that because the security expert's conduct was "relevant" Fiserv is entitled to invade attorney work product. (Dkt. 209, p. 18). This simply not the applicable standard. In order to circumvent the work product doctrine, Fiserv must demonstrate a substantial need for such discovery and "[a]s for work-product that shows 'mental impressions, conclusions, opinions, or legal theories of an attorney,' ... we have held that, 'at a minimum such material is to be protected unless a highly persuasive showing of need is made.'" *See In re Grand Jury Proceedings*, 219 F.3d at 190-91; *see also Smith v. Scottsdale Ins. Co.*, 621 F. App'x 743, 746 (4th Cir. 2015) ("Opinion work product enjoys a nearly absolute immunity and can be discovered only in very rare and extraordinary circumstances").

Here, Fiserv failed to a show substantial need for the security expert discovery—much less make the higher showing required for mental impression work product. It is undisputed that the security review occurred on a Fiserv-hosted system that Fiserv conceded it monitored and logged. (Dkt. 88 at ¶¶ 38-41). All along, Fiserv knew about the fact of the security review and Fiserv was able to have its own expert analyze the system's security controls. In other words, Fiserv already has access to the data that would provide the "individual steps" take by the security expert, as requested by Interrogatory No. 10. Thus, there is absolutely no need—let alone substantial need—

for this discovery. Additionally, the fact remains that if Fiserv wishes to inquire on Bessemer's intent in having the security review conducted, that can be addressed without invading work product protections through deposition of Bessemer's CEO.

Bessemer further objects to this recommendation based on the R&R's misapplication of the established law regarding the consulting expert privilege. FRCP 26(b)(4)(D) prohibits discovery on "facts known or opinions held by an expert retained or specially employed by another party in anticipation of litigation or to prepare for trial and who is not expected to be called as a witness at trial." As noted above, Bessemer's litigation counsel engaged the security expert in order to provide expert advice and consult during the course of litigation with Fiserv and does not expect to call the security expert as a witness at trial. The prohibition under Rule 26(b)(4)(D) therefore applies, and the R&R should have come out differently.

The R&R seeks to overrule Bessemer's consulting expert privilege objections by relying on the fact that the security expert's work is "relevant" to the claims in the case. (Dkt. 209, p. 18). Once again, this is not the test for granting an exception to the consulting expert privilege. It is well-established that a limited exception to consulting expert rule applies if Fiserv satisfies the "'heavy' burden of proving exceptional circumstances," which "exist only if defendants lack the ability to discover equivalent information by other means." *Vanguard Sav. & Loan Ass'n v. Banks*, 1995 U.S. Dist. LEXIS 2016, *9 (E.D.N.Y. 1995). Here, Fiserv does not *and cannot* allege such circumstances. As set forth above, the security review occurred on a Fiserv-hosted system, and Fiserv closely monitored and logged the security reviewer's activities. Consequently, the security expert does not possess unique knowledge about the alleged conduct that Fiserv, or one of its own experts, could not independently obtain.

Further, to the extent the Special Master relied on *Twitter, Inc. v. Musk*, 2022 WL 3656938 (Del. Ch. Aug. 25, 2022), *Twitter* is easily distinguishable. A Delaware state court decision that does not deal with Rule 26, *Twitter* relied heavily on the *pre-litigation* retention of data scientists to make business decisions regarding Musk's subsequent termination of a merger agreement. *Id.* at *5. The court also noted that Musk had relied on these experts' opinions in determining whether to terminate the agreement at issue, which later became the subject matter of the ensuing litigation. *Id*. at *6.

Here, in contrast to *Twitter*, Bessemer retained the security reviewer in September 2018, four months after it terminated its contract with Fiserv and brought suit against it. And unlike the data analysts in *Twitter*, the security reviewer had no business-related purpose prior to this litigation. Simply put, Bessemer had no prior relationship with the reviewer, and it retained the reviewer solely to provide legal advice regarding Bessemer's claims against Fiserv. (Dkt. 149, ¶¶ 13-16, 19). *Twitter* is therefore inapplicable.[4]

Lastly, the R&R also overlooks Bessemer's arguments that Fiserv's requests regarding the security reviewer are grossly disproportionate to Fiserv's the need for this discovery. The R&R's recommendation would effectively destroy Bessemer's work product and consulting expert privilege for extremely little benefit to Fiserv. Fiserv will likely use the security reviewer's identity to pursue civil claims and potential criminal prosecution. While Fiserv may claim that the security reviewer is central to its counterclaim, Fiserv's damages for its counterclaim are expected to be minimal. Above all, the discovery that Bessemer seeks to withhold is of minor importance in the context of Fiserv's resources. As noted above, Fiserv can review its own server logs and hire its

[4] The *Twitter* court also found that Twitter established "exceptional circumstances" which rendered it impracticable for Twitter to obtain relevant facts by other means. *Id*. at 7. As set forth previously, Fiserv has failed to establish any similar circumstances.

own expert. If there are any gaps to fill, Bessemer is prepared to produce any non-privileged non-work product documents and have its CEO and other personnel deposed on the subject.

Conclusion

For all the reasons set forth herein, it is respectfully requested that the Court grant the relief requested in Bessemer's motions to compel and motions for a protective order.

Dated: June 30, 2023

Respectfully submitted,

/s/ Benjamin Wilkinson

Charles J. Nerko (NY 4764338)
Kevin D. Szczepanski (NY 2720118)
Benjamin M. Wilkinson (NY 4927661)
BARCLAY DAMON LLP
80 State Street
Albany, NY 10020
(518) 429-4200
cnerko@barclaydamon.com
kzczepanski@barclaydamon.com
bwilkinson@barclaydamon.com

Richard J. Parks (PA 40477)
PIETRAGALLO, GORDON, ALFANO,
BOSICK & RASPANTI, LLP
7 West State Street, Suite 100
Sharon, PA 16146
(724) 981-1397
rjp@pietragallo.com

Counsel for Plaintiff
Bessemer System Federal Credit Union